IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Erin Drakeley O'Brien et al. Art Unit : 3628
Serial No. : 09/371,687 Examiner : Jeffrey C. Pwu
Filed : August 10, 1999
Title : PROVIDING ONE PARTY ACCESS TO AN ACCOUNT OF ANOTHER PARTY

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

(1) Real Party in Interest

FMR Corporation

(2) Related Appeals and Interferences

None known.

(3) Status of Claims

Claims 1, 3-13, 15-25, and 27-43 are pending in the case. (See Appendix of Claims.) Claims 1, 3-13, 15-25, and 27-42 were rejected under 35 U.S.C. § 102(e) as having been anticipated by U.S. 6,470,453 (hereinafter "Vilhuber"). The examiner failed to address claim 43 in the final office action dated January 16, 2004. For purposes of this appeal, the appellants assume that claim 43 also was intended to be rejected under 35 U.S.C. §102(e) as having been anticipated by Vilhuber. All of the pending claims are being appealed.

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify under 37 CFR §1.8(a) that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

9/15/04
Date of Deposit

Bethany Slack
Signature

BETHANY SLACK
Typed or Printed Name of Person Signing Certificate

(4) Status of Amendments

No amendments have been made since the final office action dated January 16, 2004.

(5) Summary of Claimed Subject Matter

The appellant's claimed subject matter relates to techniques for providing access to an account that allow one person (sometimes called a "pretender") to access to another person's (sometimes called an "owner") account without the pretender knowing an authenticator (e.g., a password) of the owner's. [specification, page 1, lines 6-7, 25-26]

For example, a pretender may be a customer service representative employed by the investment company that manages the owner's account, and, may receive a call from the account owner seeking assistance with his or her account. By using the access techniques disclosed in the specification, the customer service representative can assist the owner by accessing the owner's account without having to obtain a sensitive password from the owner. [specification, pages 1-2, lines 26-28, 1-2]

Claims 1, 13 and 25 are directed to a method, a computer program product, and an apparatus, respectively, that provide access to an account of a second party (e.g., the owner). The claims recite identification information associated with a first party that does not contain an authenticator of the second party (e.g., the owner) [specification, page 7, lines 15-17; FIGs. 1-5]; based on the identification information, receiving account information that defines a right of the first party to access account data associated with the account of the second party [specification, page 7, lines 20-30; FIGs. 1-5]; and enabling the first party to access the account data based on the account information, without receiving the authenticator (e.g., password) of the second party [specification, page 8, line 18 – page 9, line 13; FIGs. 1-5].

Claims 9, 21, and 33 are directed to a method, a computer program product, and an apparatus, respectively, that provide a first party with access to an account of a second party. The method includes receiving identification information associated with the first party that does not contain an authenticator of the second party [specification, page 7, lines 15-17; FIGs. 1-5]; verify that the first party is entitled to access account data associated with the account of the second party based on the identification information and account information that defines a right of the first party to access the account data [specification, page 7, lines 20-30, page 8, lines 18-

23; FIGs. 1-5]; and provide the account information to a storage device associated with the first party for use in accessing the account data, wherein the account information does not contain the authenticator of the second party [specification, page 9, lines 5-13; FIGs. 1-5].

Claims 40, 41, and 42 are directed to a method, a computer program product, and an apparatus, respectively, implementing techniques for providing access to an account of a second party. The method includes receiving identification information associated with a first party that does not contain an authenticator of the second party [specification, page 7, lines 15-17; FIGs. 1-5]; based on the identification information, providing account information that defines a right of the first party to access account data associated with the account of the second party [specification, page 7, lines 20-30; FIGs. 1-5]; and permitting access to the account data by the first party based on the account information, without receiving the authenticator of the second party [specification, page 8, line 18 – page 9, line 13; FIGs. 1-5].

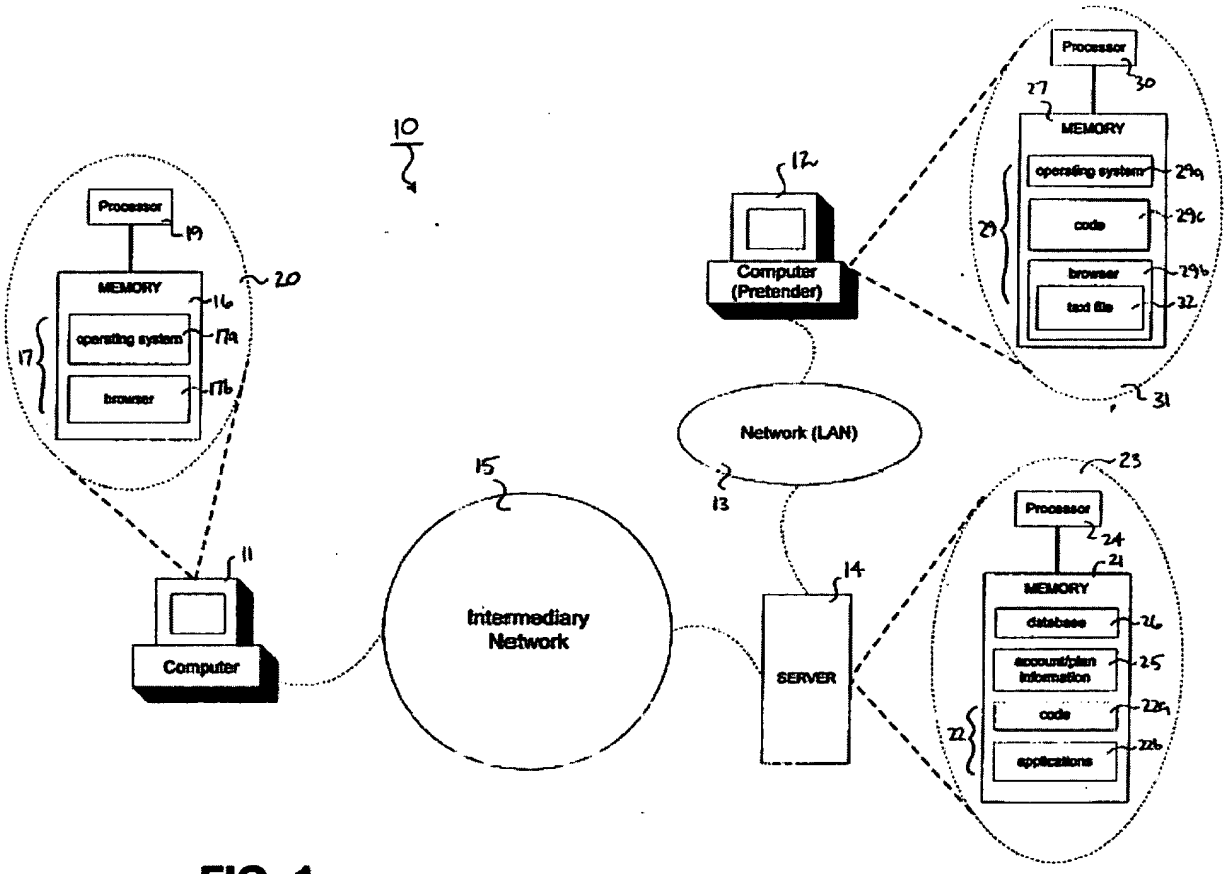


FIG. 1

As illustrated in the example shown in Fig. 1 of the application, a pretender provides, through a client computer 12, a user identifier and password (assigned to the pretender) to a server 14. [specification, page 7, lines 15-17] The server 14 authenticates the pretender based on user identifier and password information stored in a database 26, and retrieves access information from the database 26 that corresponds to the pretender's user identifier and password. [specification, page 7, lines 20-27] The retrieved access information identifies which applications 22b (e.g., Plan Sponsor Webstation® and NetBenefits® available from Fidelity® Investments) are accessible to the pretender. [specification, page 7, lines 27-30]

The server 14 provides the access information to the pretender's client computer 12, where the access information is stored in a text file 32. [specification, page 7, line 31 – page 8, line 11] The server 14 also provides a web page 39 (FIG. 5 reproduced below) to the pretender's client computer 12. [specification, page 7, lines 32-33]

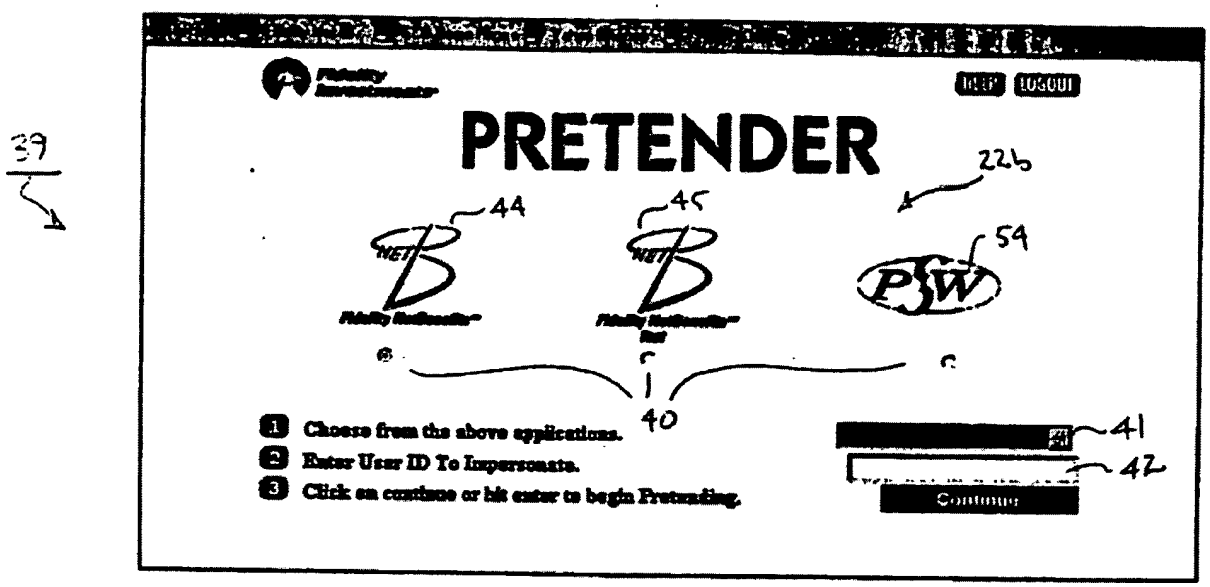


FIG. 5

By using the web page 39, the pretender can select a particular application 22b (e.g., Plan Sponsor Webstation® or NetBenefits®), and enter a user identifier (assigned to a person other than the pretender e.g., a customer) into an entry box 42 on the web page 39. [specification, page 8, lines 12-15] The user identifier that is entered into the entry box 42 corresponds to an account the pretender wants to access from the selected application. [specification, page 8, lines 14-15]

It is significant that the web page 39 only requires the pretender to enter a user identifier corresponding to an account that the pretender wants access to and not a password.

The server 14 verifies that the pretender is permitted to access the account associated with the user identifier that was entered in the entry box 42. [specification, page 8, lines 18-23] If the pretender is permitted to access the account, the server 14 retrieves account information associated with the account. [specification, page 8, lines 23-27] The retrieved account information identifies which programs (e.g., a program to obtain account balances, or a program to obtain market indices) the pretender is permitted to access, and the restrictions, if any, on the pretender's right to view data, execute programs, and change parameters of the account. [specification, page 8, line 28 – page 9, line 4]

The server 14 provides the account information to the pretender's client computer 12, where the account information is stored in the text file 32 along with the access information. [specification, page 9, lines 5-8] The access information and account information in the text file 32 are used to gain access to accounts and applications. [specification, page 9, lines 8-10] For example, if the pretender selects applications 44 or 45 from the web page 39 (FIG. 5), and inputs a user identifier in the entry box 42, the server 14 provides the web page 46 (FIG. 6 reproduced below) to the pretender's client computer 12. [specification, page 9, lines 10-13]

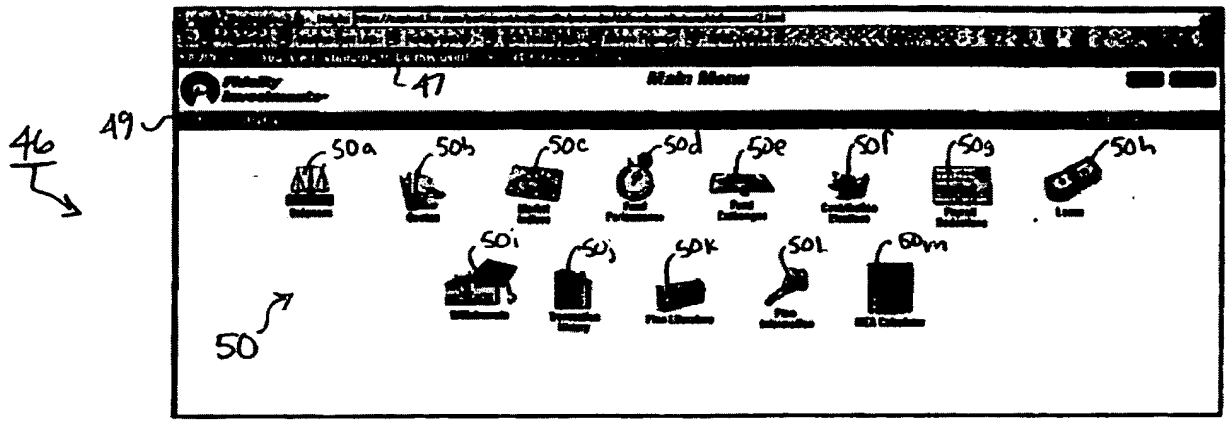


FIG. 6

The web page 46 displayed to the pretender includes the same information that is displayed to the owner of the account whose user identifier was entered into the entry box 42. [specification, page 9, lines 13-15] The web page 46 also includes an indication 47 that the pretender is "pretending" to be the owner whose user identifier ID was specified in the entry box 42. [specification, page 9, lines 15-18]

In this example an owner is a person who owns funds in an investment account. [specification, page 4, lines 24-25] The owner can access the account by providing a user identifier and password (assigned to the owner) to a server. [specification, page 1, lines 12-14] Once the owner has access to the account, the owner can access programs and/or databases in order to view account information (e.g., balances) or change account parameters (e.g., fund allocations). [specification, page 1, lines 14-16]

A pretender is, for example, a person authorized to access at least one other person's account without knowing that person's password for the account. [specification, page 4, lines 17-19] For example, an employee of an investment firm can access a retirement or investment plan of a company, an individual account in such a plan, or an independent account of a private investor. [specification, page 4, lines 19-22] Once the pretender has access to the account, the programs and/or databases that the owner of the account has access to are displayed to the pretender. [specification, page 4, lines 22-24]

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1, 3-13, 15-25, and 27-43 stand rejected under 35 U.S.C. 102(e) as being anticipated by Vilhuber.

(7) Argument

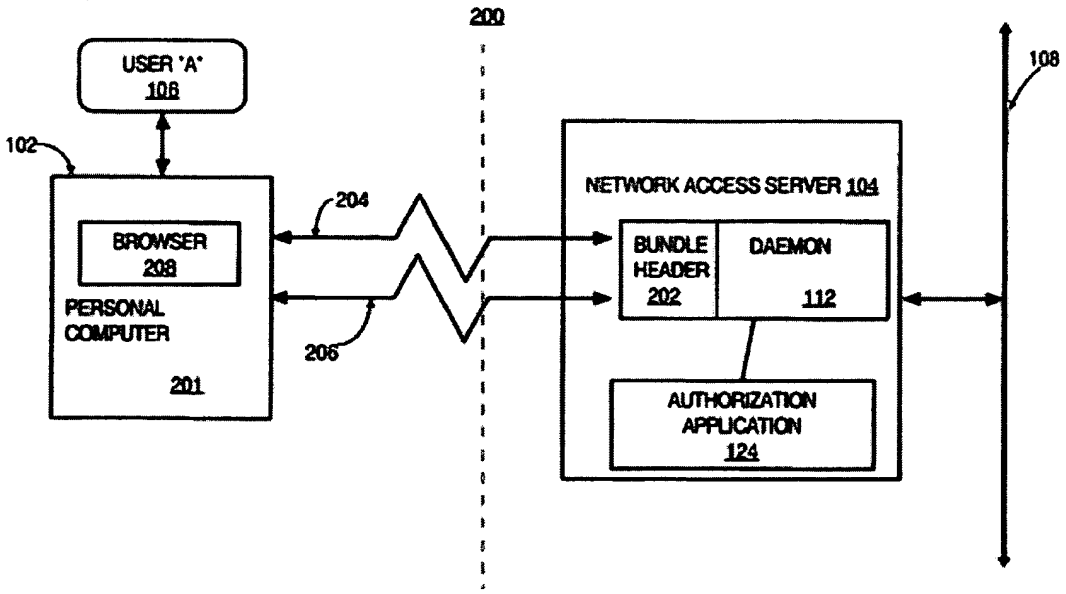
For a reference to anticipate a claim, each element and limitation of the claim must be found in the reference. *Hoover Group, Inc. v. Custom Metalcraft, Inc.*, 66 F.3d 299, 302 (Fed. Cir. 1995). Vilhuber does not disclose all of the elements of the claims.

Vilhuber

Vilhuber's system authenticates multiple connections from a client computer to a server computer. [Vilhuber, abstract] The connections referred to in Vilhuber are dial-in protocol connections, such as Point to Point Protocol (PPP) connections and Serial Line Internet Protocol (SLIP) connections. [Vilhuber, col. 7, lines 5-18] Vilhuber explains that one problem with using dial-in protocols is that when a client computer connected to a server by a first connection requests additional connections to the server, the protocol treats the additional connections as separate connections during the client authentication and authorization phases. [Vilhuber, col. 8, lines 49-53] This results in the user at the client computer having to reenter a valid user name and password each time an additional connection is made between the client computer and the server computer. [Vilhuber, col. 8, lines 53-56] Vilhuber proposes to solve this problem by having the server computer automatically assign each subsequent connection the set of user privileges that was assigned to the first connection. [Vilhuber, col. 9, lines 28-38]

The basic architecture of the Vilhuber system is shown in its FIG. 2, which is reproduced below:

FIG. 2



To establish a first connection 204 between the client computer 102 and the server computer 104, the server computer 104 performs a client authentication phase to determine whether the client computer 102 is allowed to maintain a connection with the server computer 104. [Vilhuber, col. 7, lines 60-63] If the client computer 102 is authenticated, the server computer 104 performs a client authorization phase to identify a set of client privileges for the first connection 204 based on certain attributes of the client computer 102. [Vilhuber, col. 5, lines 48-52] The identified set of client privileges is then assigned to the first connection 204. [Vilhuber, col. 8, lines 1-3]

Once the first connection is authenticated and authorized, the server computer 104 performs a user authentication phase to determine whether a particular user 106 at the client computer 102 is allowed to access the server computer 104. [Vilhuber, col. 8, lines 4-7] During the user authentication phase, the user 106 provides user access information (in the form of a user name and password, a Smart card, or a Token card) to the server computer 104. [Vilhuber, col. 8, lines 8-10, lines 28-37] Once the identity of the user 106 is authenticated, the server computer 104 performs a user authorization phase and assigns a set of user privileges (based on

the user's access information) to the first connection 204. [Vilhuber, col. 8, lines 21-23] The set of user privileges assigned to the first connection overrides the previously-assigned set of client privileges. [Vilhuber, col. 8, lines 23-25] The user privileges specify which devices and resource on the network 108 the user 106 has access to. [Vilhuber, col. 5, line 66 – col. 6, lines 2]

When the server computer 104 receives a request from the client computer 102 to establish an additional connection 206, the server computer 104 automatically assigns to the second connection 206 the same set of user privileges that were previously-assigned to the first connection 204. [Vilhuber, col. 6, lines 6-14] The server computer 104 does not repeat the client authorization phase or the user authentication and authorization phases. [Vilhuber, col. 6, lines 14-18]

Group I (claims 1, 13, 25, 37, 38, 39 and 43)

For the purposes of this appeal only, claims 1, 13, 25, 37, 38, 39 and 43 may be treated as rising and falling together. Claim 1, which is representative of this group, recites:

> **1. A computer-implemented method for providing access to an account of a second party, comprising:**
> **receiving identification information associated with a first party that does not contain an authenticator of the second party;**
> **based on the identification information, receiving account information that defines a right of the first party to access account data associated with the account of the second party; and**
> **enabling the first party to access the account data based on the account information, without receiving the authenticator of the second party.**

In claim 1, what the first party is provided access to is account data of a second party, and that access is provided without receiving the authentication of the second party. In Vilhuber, by contrast, the user privileges relate to device and resources on the network. Vilhuber's system says nothing about a first party (e.g., an investment fund employee) being given to access to a second party's (e.g., an account holder) account data, let alone getting such access without receiving an authenticator of the second party. Indeed, there is no mention in Vilhuber of a user gaining access to any account, much less a user gaining access to another user's account.

The examiner's argument is reproduced below:

> **Vilhuber discloses a computer-implemented system, method, and apparatus for providing access to an account of a second party substantially claimed including:**

receiving identification information associated with a first party (client first connection) that does not contain an authenticator of the second party (second connection);

based on the identification information, receiving an account information that defines a right of the first party to access account data associated with the account of the second party (316);

accessing the account information of the second party based on the account information session manager (124); and

enabling the first party to access the account of the second party based on the account information (abstract).

As a preliminary matter, the examiner has included in his argument a claim limitation that is not recited in claim 1, namely "accessing the account information of the second party based on the account information session manager". Because this limitation is not included in the claims of Group I, we do not address it in this section.

The examiner takes an untenable position in an attempt to link Vilhuber to the claims, implying that the "first connection" in Vilhuber corresponds to the "first party" in claim 1, and the "second connection" in Vilhuber corresponds to the "second party" in claim 1. This construction of the term "party" is not supported by its ordinary meaning or the way the term is used in the specification.[1]

The appellant's specification used the term "party" consistently with its ordinary meaning (1) a person or group participating in an action or affair; or (2) a particular individual. [Merriam-Webster Dictionary, www.m-w.com, last visited on 3/9/2004]

In the specification, the second party is, for example, an owner of an investment account and the first party is, for example, an employee of an investment firm who makes investment decisions for the account. [*See, e.g.,* specification, page 4, lines 17-28]

Moreover, Vilhuber does not use the term "connection" in any special way that would cause a person of ordinary skill in the art to equate it with "party." In Vilhuber, the connections are communication channels. Vilhuber mentions a Point to Point Protocol (PPP) connection and a Serial Line Internet Protocol (SLIP) connection as examples of connection that are used to exchange information between a client computer and a server computer. [*See, e.g.,* Vilhuber, col. 7, lines 5-17] Such connections are not parties and the appellant respectfully submits that the examiner has attributed to "party" a meaning that conflicts with common English and the text

[1] Absent a special and particular definition created by the patent application, terms in a claim are to be given their ordinary and accustomed meaning. *Renishaw PLC v. Marposs Societa Per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998).

of Vilhuber by contending that a "connection" is a "party". If "party" is construed according to its plain and ordinary meaning, there is no link between Vilhuber and the Group I claims.

Even if "party" could somehow be construed to encompass a "connection", Vilhuber nonetheless fails to disclose several claims elements of Group I, including: (1) the "identification information associated with a first party"; (2) the "authenticator of the second party"; (3) the "account information"; (4) the "account data"; and (5) the "account of the second party".

Indeed, the examiner's argument offers no explanation as to how Vilhuber discloses these claim elements. Rather, the examiner makes a broad-brush argument that (i) "box 316" of Vilhuber discloses the entire claim limitation "based on the identification information, receiving account information that defines a right of the first party to access account data associated with the account of the second party" and (ii) Vilhuber's Abstract discloses the entire claim limitation "enabling the first party to access the account data based on the account information, without receiving the authenticator of the second party". For convenience, we reproduce below the text of Vilhuber corresponding to box 316 and the Abstract:

> **"As shown by block 316, a user authentication phase is performed to determine whether the user is authorized to connect to the network access server. To perform the user authentication phase, the user is required to provide user access information that is used by the authorization application to determine if the user should be allowed to connect to the network access server." [Vilhuber, col. 11, lines 6-24]**
>
> **"A mechanism for authenticating multiple connections to a network server is disclosed. A client establishes a first connection to the server. In establishing the first connection, the client provides authentication information and authorization information, and in response the server assigns first access privileges to the client. When the client requests a second connection, the server receives authentication information from the client, and assigns limited access privileges to the client. The server associates the first connection with the second connection and the client. The server automatically associates the first access privileges with the second connection, without requiring the client to provide authorization information for the second connection." [Vilhuber, Abstract]**

With respect to Vilhuber's disclosure relating to "block 316", Vilhuber discloses an authorization application that receives a party's access information (e.g., user name and password) to determine whether to provide the party access to a network access server. There is nothing in Vilhuber's description of block 316 to suggest that that the authorization application also receives account information that defines a right of the party to access another party's account data based on the identification of the party as required by the claims of Group I.

With respect to the disclosure of the Vilhuber abstract, while Vilhuber discloses that a server does not require a client computer to provide its authorization information when the client computer establishes a second connection with the client computer, there is nothing to suggest that the client computer is enabled through the second connection "to access ... account data based on ... account information" that defines a right of the first party to access account data associated with the account of the second party. Moreover, it is clear that the "authorization information" in Vilhuber is information associated with the user of the client computer that establishes a first and second connection to the server, and is not an authenticator of a different user as in the claims of Group I.

For at least these reasons, the appellant respectfully submits that the claims of Group I should be allowed.

Group II (claims 9, 21, and 33)

For the purposes of this appeal only, claims 9, 21, and 33 may be treated as rising and falling together. Claim 9, which is representative of this group, recites:

> **9. A method of providing a first party with access to an account of a second party, comprising:**
> **receiving identification information associated with the first party that does not contain an authenticator of the second party;**
> **verifying that the first party is entitled to access account data associated with the account of the second party based on the identification information and account information that defines a right of the first party to access the account data; and**
> **providing the account information to a storage device associated with the first party for use in accessing the account data,**
> **wherein the account information does not contain the authenticator of the second party.**

The examiner has not indicated which elements of Vilhuber correspond to the limitations of claim 9. The appellant is assuming, for the sake of argument, that the examiner has made the correspondences set forth in the following table:

Claim 9	**Vilhuber**
first party	first connection
second party	second connection
identification information	user access information
account information	user access privileges
authenticator of the second party	authorization information for the second connection

Based on these assumptions, claim 9 (with the appropriate substitutions in italic-face type) would read as follows:

> **A method of providing a *first connection* with access to an account of a *second connection*, comprising:**
>
> **receiving user access information that does not contain authorization information for the second connection;**
>
> **verifying that the *first connection* is entitled to access account data associated with the account of the *second connection* based on the *user access information* and *user access privileges* that defines a right of the *first connection* to access the account data; and**
>
> **providing the *user access privileges* to a storage device associated with the *first connection* for use in accessing the account data,**
>
> **wherein the user access privileges does not contain the authorization information for the second connection.**

Even with such an interpretation of the limitations of claim 9, there is still nothing in Vilhuber to suggest that the first connection or the second connection have accounts. Accordingly, there was no need for Vilhuber to have disclosed verifying that the "first connection" is entitled to access account data associated with the account of the "second connection" based on the "user access information and user access privileges".

Further, the user access privileges in Vilhuber do not appear to be provided to any component of the Vilhuber system. Vilhuber describes the server 104 as including an Authorization application 124, which is "a back-end server-side mechanism that is used to determine whether a particular user is authorized to access the network 108 through network access server 104." [Vilhuber, col. 7, lines 19-22] Vilhuber discloses one embodiment in which once a first "telnet connection is established, the authorization application 124 runs an access profile command that causes the first connection 204 to inherit the set of user access privileges. The appellant contends that even if the "user access privileges" in Vilhuber correspond to the "account information" of claim 9, Vilhuber still does not disclose providing the "user access privileges" to a storage device associated with the "first connection" for use in accessing the account data.

Group III (claims 40, 41, and 42)

For the purposes of this appeal only, claims 40, 41, and 42 may be treated as rising and falling together. Claim 40, which is representative of this group, recites:

1. A computer-implemented method for providing access to an account of a second party, comprising:
receiving identification information associated with a first party that does not contain an authenticator of the second party;
based on the identification information, providing account information that defines a right of the first party to access account data associated with the account of the second party; and
permitting access to the account data by the first party based on the account information, without receiving the authenticator of the second party.

The examiner has not indicated which elements of Vilhuber correspond to the limitations of claim 40. The appellant is assuming, for the sake of argument, that the examiner has made the correspondences set forth in the following table:

Claim 40	Vilhuber
first party	first connection
second party	second connection
identification information	user access information
account information	user access privileges
authenticator of the second party	authorization information for the second connection

If the appellant's assumptions are accurate, claim 40 (with the appropriate substitutions in italic-face type) would read as follows:

40. A computer-implemented method for providing access to an account of a *second connection*, comprising:
receiving user access information associated with a first connection that does not contain authorization information for the second connection;
based on the *user access information*, providing *user access privileges* that defines a right of the *first connection* to access account data associated with the account of the *second connection*; and
permitting access to the account data by the *first connection* based on the *user access privileges*, without receiving the *authorization information for the second connection*.

Even with such an interpretation of the limitations of claim 40, there is still nothing in Vilhuber to suggest that the first connection or the second connection have accounts. At most, an argument could be made that a user has an account (associated with the user's identification information) on the server in Vilhuber. Even so, Vilhuber says nothing about "providing account information" that defines a right of the user to access an account of any other user. Rather, Vilhuber discloses assigning user access privileges that define a right of the user to access network devices and network resources through the server.

Group IV (claims 3, 15, and 27)

For the purposes of this appeal only, claims 3, 15, and 27 may be treated as rising and falling together. Claim 3, which is representative of this group, recites:

> **3. The method of claim 1, further comprising storing the account information in a text file;**
> **wherein enabling further comprises:**
> **receiving, from the first party, a request to access the account data;**
> **receiving an interrogation into the text file from software that controls access to the account data; and**
> **enabling access to the account data if the software determines, based on the interrogation, that the first party is entitled to access the account data.**

Vilhuber does not disclose these features. The examiner has failed to identify where Vilhuber teaches or suggests storing account information in a text file, much less receiving an interrogation into the text file from software that controls access to the account data. Vilhuber does not disclose at least these features of claims 3, 15 and 27.

Group V (claims 4, 16, and 28)

For the purposes of this appeal only, claims 4, 16, and 28 may be treated as rising and falling together. Claim 4, which is representative of this group, recites:

> **4. The method of claim 3, wherein the text file comprises an Internet cookie, the method further comprising,**
> **inputting, by the first party, the identification information on a Web page accessed by a Web browser.**

Vilhuber does not disclose these features. The examiner has failed to identify where Vilhuber teaches or suggests a text file comprising an Internet cookie, much less inputting identification information on a Web page accessed by a Web browser. Vilhuber does not disclose at least these features of claims 4, 16, and 28.

Group VI (claims 5, 6, 17, 18, 29 and 30)

For the purposes of this appeal only, claims 5, 6, 17, 18, 29 and 30 may be treated as rising and falling together. Claim 5, which is representative of this group, recites:

> **5. The method of claim 1, further comprising:**
> **receiving information identifying the first party;**
> **receiving access information that corresponds to the information identifying the first party, the access information defining a right of the first party to access a program that controls access to the account data; and**

providing access to the program based on the access information.

Vilhuber does not disclose these features. The examiner has failed to identify where Vilhuber teaches or suggests receiving access information defining a right of the first party to access a program that controls access to the account data, much less providing access to the program based on the access information. Vilhuber does not disclose at least these features of claims 5, 6, 17, 18, 29 and 30.

Group VII (claims 7, 19, and 31)

For the purposes of this appeal only, claims 7, 19, and 31 may be treated as rising and falling together. Claim 7, which is representative of this group, recites:

7. The method of claim 1, further comprising displaying information corresponding to the account data.

Vilhuber does not disclose this feature. The examiner has failed to identify where Vilhuber teaches or suggests account data, much less displaying information corresponding to the account data. Vilhuber does not disclose at least this feature of claims 7, 19, and 31.

Group VIII (claims 8, 20, and 32)

For the purposes of this appeal only, claims 8, 20, and 32 may be treated as rising and falling together. Claim 8, which is representative of this group, recites:

8. The method of claim 1, further comprising changing a parameter associated with the account data.

Vilhuber does not disclose this feature. The examiner has failed to identify where Vilhuber teaches or suggests account data, much less changing a parameter associated with the account data. Vilhuber does not disclose at least this feature of claims 8, 20, and 32.

Group IX (claims 10, 22, and 34)

For the purposes of this appeal only, claims 10, 22, and 34 may be treated as rising and falling together. Claim 10, which is representative of this group, recites:

10. The method of claim 9, further comprising:
receiving a request from the first party to access the account data;
obtaining the account information from the storage device associated with the first party; and

determining whether the first party is entitled to access the account data based on the account information.

Vilhuber does not disclose these features. The examiner has failed to identify where Vilhuber teaches or suggests account data or a storage device associated with the first party. Accordingly, there is no reason for Vilhuber to disclose obtaining the account information from the storage device associated with the first party, much less determining whether the first party is entitled to access the account data based on the account information. Vilhuber does not disclose at least these features of claims 10, 22, and 34.

Group X (claims 11, 12, 23, 24, 35, and 36)

For the purposes of this appeal only, claims 11, 12, 23, 24, 35, and 36 may be treated as rising and falling together. Claim 11, which is representative of this group, recites:

11. The method of claim 9, further comprising:
receiving information identifying the first party;
verifying that the first party is entitled to access a program that controls access to the account data based on the information identifying the first party; and
providing access information to the storage device associated with the first party for use in accessing the program.

Vilhuber does not disclose these features. The examiner has failed to identify where Vilhuber teaches or suggests verifying that the first party is entitled to access a program that controls access to the account data based on the information identifying the first party, much less providing access information to the storage device associated with the first party for use in accessing the program. Vilhuber does not disclose at least these features of claims 11, 12, 23, 24, 35, and 36.

Enclosed is a $330 check for the brief fee and a $950 check for the Petition for Extension of time fee. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 9/15/04

Mandy Jubang
Reg. No. 45,884

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

20935489.doc

Appendix of Claims

Claim 1. A computer-implemented method for providing access to an account of a second party, comprising:

receiving identification information associated with a first party that does not contain an authenticator of the second party;

based on the identification information, receiving account information that defines a right of the first party to access account data associated with the account of the second party; and

enabling the first party to access the account data based on the account information, without receiving the authenticator of the second party.

Claim 2. (cancelled)

Claim 3. The method of claim 1, further comprising storing the account information in a text file;

wherein enabling further comprises:

receiving, from the first party, a request to access the account data;

receiving an interrogation into the text file from software that controls access to the account data; and

enabling access to the account data if the software determines, based on the interrogation, that the first party is entitled to access the account data.

Claim 4. The method of claim 3, wherein the text file comprises an Internet cookie, the method further comprising,

inputting, by the first party, the identification information on a Web page accessed by a Web browser.

Claim 5. The method of claim 1, further comprising:

receiving information identifying the first party;

receiving access information that corresponds to the information identifying the first party, the access information defining a right of the first party to access a program that controls access to the account data; and

providing access to the program based on the access information.

Claim 6. The method of claim 5, wherein providing access further comprises providing access to the first party based on the access information and the account information.

Claim 7. The method of claim 1, further comprising displaying information corresponding to the account data.

Claim 8. The method of claim 1, further comprising changing a parameter associated with the account data.

Claim 9. A method of providing a first party with access to an account of a second party, comprising:

receiving identification information associated with the first party that does not contain an authenticator of the second party;

verifying that the first party is entitled to access account data associated with the account of the second party based on the identification information and account information that defines a right of the first party to access the account data; and

providing the account information to a storage device associated with the first party for use in accessing the account data,

wherein the account information does not contain the authenticator of the second party.

Claim 10. The method of claim 9, further comprising:

receiving a request from the first party to access the account data;

obtaining the account information from the storage device associated with the first party; and

determining whether the first party is entitled to access the account data based on the account information.

Claim 11. The method of claim 9, further comprising:

receiving information identifying the first party;

verifying that the first party is entitled to access a program that controls access to the account data based on the information identifying the first party; and

providing access information to the storage device associated with the first party for use in accessing the program.

Claim 12. The method of claim 11, further comprising:

receiving a request from the first party to access the program;

obtaining the access information from the storage device associated with the first party; and

determining whether the first party is entitled to access the program based on the access information and the account information.

Claim 13. A computer program stored on a computer-readable medium for providing access to an account of a second party, the computer program comprising instructions that cause a computer to:

receive identification information associated with a first party that does not contain an authenticator of the second party;

based on the identification information, receive account information that defines a right of the first party to access account data associated with the account of the second party; and

enable the first party to access the account data based on the account information, without receiving the authenticator of the second party.

Claim 14. (cancelled)

Claim 15. The computer program of claim 13, further comprising instructions that cause the computer to:

store the account information in a text file;

receive a request from the first party to access the account data;

receive an interrogation into the text file from software that controls access to the account data; and

enable access to the account if the software determines, based on the interrogation, that the first party is entitled to access the account data.

Claim 16. The computer program of claim 15, wherein:

the first party inputs the identification information on a Web page accessed by a Web browser; and

the text file comprises an Internet cookie.

Claim 17. The computer program of claim 13, further comprising instructions that cause the computer to:

receive information identifying the first party;

receive access information that corresponds to the information identifying the first party, the access information defining a right of the first party to access a second program that controls access to the account data; and

provide access to the second program based on the account information.

Claim 18. The computer program of claim 17, wherein instructions that cause a computer to provide access further comprise instructions that cause a computer to provide access to the first party based on the access information and the account information.

Claim 19. The computer program of claim 13, further comprising instructions to cause the computer to display information corresponding to the account data.

Claim 20. The computer program of claim 13, further comprising instructions to cause the computer to change a parameter associated with the account data.

Claim 21. A computer program stored on a computer-readable medium for providing a first party with access to an account of a second party, the computer program comprising instructions that cause a computer to:

receive identification information associated with the first party that does not contain an authenticator of the second party;

verify that the first party is entitled to access account data associated with the account of the second party based on the identification information and account information that defines a right of the first party to access the account data; and

provide the account information to a storage device associated with the first party for use in accessing the account data,

wherein the account information does not contain the authenticator of the second party.

Claim 22. The computer program of claim 21, further comprising instructions that cause the computer to:

receive a request from the first party to access the account data;

obtain the account information from the storage device associated with first party; and

determine whether the first party is entitled to access the account data based on the account information.

Claim 23. The computer program of claim 21, further comprising instructions that cause the computer to:

receive information identifying the first party;

verify that the first party is entitled to access second program that controls access to the account data based on the information identifying the first party; and

provide access information to the storage device associated with the first party for use in accessing the second program.

Claim 24. The computer program of claim 23, further comprising instructions that cause the computer to:

receive a request from the first party to access the second program;

obtain the access information from the storage device associated with the first party; and

determine whether the first party is entitled to access the second program based on the access information and the account information.

Claim 25. An apparatus for providing access to an account of a second party, comprising:

a memory which stores computer instructions; and

a processor which executes the instructions to (i) receive identification information associated with a first party that does not contain an authenticator of the second party, (ii) based on the identification information, receive account information that defines a right of the first party to access account data associated with the account of the second party, and (iii) enable access to the account data based on the account information, without receiving the authenticator of the second party.

Claim 26. (cancelled)

Claim 27. The apparatus of claim 25, wherein the processor executes instructions to (i) store the account information in a text file, (ii) receive a request from the first party to access the account data, (iii) receive an interrogation into the text file from software that controls access to the account data, and (iv) receive access to the account data if the software determines, based on the interrogation, that the first party is entitled to access the account data.

Claim 28. The apparatus of claim 27, wherein:

the first party inputs the identification information on a Web page accessed by a Web browser; and

the text file comprises an Internet cookie.

Claim 29. The apparatus of claim 25, wherein:

the processor executes instructions to (i) receive information identifying the first party, (ii) receive access information that corresponds to the information identifying the first party, the access information defining a right of the first party to access a program that controls access to the account data, and (iii) provide access to the program based on the access information.

Claim 30. The apparatus of claim 29, wherein the processor is further configured to provide access to the first party based on the access information and the account information.

Claim 31. The apparatus of claim 25, wherein the processor executes instructions to display information corresponding to the account data.

Claim 32. The apparatus of claim 25, further comprising changing a parameter associated with the account data.

Claim 33. An apparatus for providing a first party with access to an account of a second party, comprising:

a memory which stores computer instructions; and

a processor which executes the instructions to (i) receive identification information associated with the first party that does not contain an authenticator of the second party, (ii) verify that the first party is entitled to access account data associated with the account of the second party based on the identification information and account information that defines a right of the first party to access the account data, and (iii) provide the account information to a storage device associated with the first party for use in accessing the account data,

wherein the account information does not contain the authenticator of the second party.

Claim 34. The apparatus of claim 33, wherein the processor executes instructions to (i) receive a request from the first party to access the account data, (ii) obtain the account information from the storage device associated with the first party, and (iii) determine whether the first party is entitled to access the account data based on the account information.

Claim 35. The apparatus of claim 33, wherein the processor executes instructions to (i) receive information identifying the first party, (ii) verify that the first party is entitled to access a program that controls access to the account data based on the information identifying the first party, and (iii) provide access information to the storage device associated with the first party for use in accessing the program.

Claim 36. The apparatus of claim 35, wherein the processor executes instructions to (i) receive a request from the first party to access the program, (ii) obtain the access information from the storage device associated with the first party, and (iii) determine whether the first party is entitled to access the program based on the access information and the account information.

Claim 37. The method of claim 1, wherein the account of the second party is accessed over an intranet running HTTPS.

Claim 38. The computer program of claim 13, wherein the account of the second party is accessed over an intranet running HTTPS.

Claim 39. The apparatus of claim 25, wherein the account of the second party is accessed over an intranet running HTTPS.

Claim 40. A computer-implemented method for providing access to an account of a second party, comprising:

receiving identification information associated with a first party that does not contain an authenticator of the second party;

based on the identification information, providing account information that defines a right of the first party to access account data associated with the account of the second party; and

permitting access to the account data by the first party based on the account information, without receiving the authenticator of the second party.

Claim 41. A computer program stored on a computer-readable medium for providing access to an account of a second party, the computer program comprising instructions that cause a computer to:

receive identification information associated with a first party that does not contain an authenticator of the second party;

based on the identification information, provide account information that defines a right of the first party to access account data associated with the account of the second party; and

permit access to the account data by the first party based on the account information, without receiving the authenticator of the second party.

Claim 42. An apparatus for providing access to an account of a second party, comprising:

a memory which stores computer instructions; and

a processor which executes the instructions to (i) receive identification information associated with a first party that does not contain an authenticator of the second party, (ii) based on the identification information, provide account information that defines a right of the first party to access account data associated with the account of the second party, and (iii) permit access to the account data by the first party based on the account information without receiving the authenticator of the second party.

Claim 43. The method of claim 1, wherein the authenticator is a password.